**NEW ZEALAND**

# Porirua City Council and Whangarei District Council websites cryptojacked in internation cyber attack

14 Feb, 2018 1:41pm

4 minut

Hackers hit more than 4000 websites around the world, injecting a crypto mining code into scripts being used on their sites. Photo / 123RF

NZ Herald
By: **Chris Knox** and **Melissa Nightingale**

At least two council websites fell victim to cryptojackers last weekend without anybody realising, leaving visitors to the sites unwittingly helping hackers mine for cryptocurrency.

The Porirua City Council and Whangarei District Council are among several thousand sites internationally that were caught up in what Netsafe has called a "benign" attack.

Porirua City Council's chief information officer Steve McIntosh said the website itself was not compromised. But anyone visiting the site during the attack downloaded malicious code without realising it.

On Sunday, 4275 websites, including the US Courts site and the UK's Information Commissioner's Office site were running a script that had been altered to add a Coinhive crypto miner to any page it was loaded into.

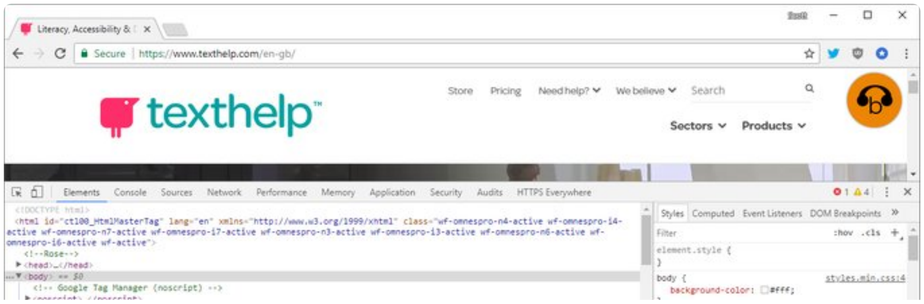
"People who visited that website over the weekend, they would have seen their CPU, the brains of their computers, spike up to an enormous amount of activity suddenly," said Netsafe's director of technology Sean Lyons.

**Scott Helme** @Scott_Helme 11 Feb
Replying to @Scott_Helme
Ok so this is via a 3rd party compromise, here is the script:
browsealoud.com/plus/scripts/b…

**Scott Helme**
@Scott_Helme

Hey @texthelp you've been compromised, you need to address this ASAP. Their site also has the crypto miner running: pic.twitter.com/fl0U9ssZRr

10:16 PM - Feb 11, 2018



```
<!DOCTYPE html>
<html id="ctl00_HtmlMasterTag" lang="en" xmlns="http://www.w3.org/1999/xhtml" class="wf-omnespro-n4-active wf-omnespro-i4-active wf-omnespro-n7-active wf-omnespro-i7-active wf-omnespro-n3-active wf-omnespro-i3-active wf-omnespro-n6-active wf-omnespro-i6-active wf-active">
  <!--Rose-->
  ▶<head>…</head>
...▼<body> == $0
    <!-- Google Tag Manager (noscript) -->
```

```
element.style {
}
body {                                  styles.min.css:4
  background-color: □#fff;
```

105    43 people are talking about this

"They were being used to mine cryptocurrency without their knowledge, without their host's knowledge."

The practice is called "cryptojacking" and is when hackers use people's computers to "build small parts of cryptocurrency" such as Bitcoin.

The hack was "at the benign end of what could happen".

"What people are doing is they're using your processing power, they're using your computer, albeit for a short space of time, as part of a giant hive of computers to help them generate money."

Visitors to the Porirua City Council website on Sunday may have noticed their devices were running slower as they mined for cryptocurrency, similar to Bitcoin. Photo / 123RF

Affected people would discover their devices were running "massively slow" while they were on the site.

"Often people wouldn't notice. People would just say 'I wonder why my fans have started running' or 'I wonder why my computer's slowed down'."

In theory if they stayed on the site long enough their CPU could overheat and cause physical damage to the computer, but that was unlikely, he said.

After being contacted by the *Herald*, a council spokeswoman said on Tuesday that as far as they were aware, the website had not been cryptojacked.

But screenshots show the site was still running the compromised script yesterday, a text-to-speech accessibility script called BrowseAloud by TextHelp.com. Security researcher Scott Helme posted on Twitter, saying it appeared the script was altered between about 3am and 1.20pm on Sunday (GMT).

The script was no longer on the council site this morning.

> **Scott Helme**
> @Scott_Helme
>
> It seems like the @texthelp script file was modified between Sun, 11 Feb 2018 02:58:04 GMT and Sun, 11 Feb 2018 13:21:56 GMT according to the @internetarchive:web.archive.org/web/2018021102…web.archive.org/web/2018021113…
>
> 1:04 AM - Feb 12, 2018
>
> 7 See Scott Helme's other Tweets

"Our website was not compromised in any way," McIntosh said in a statement.

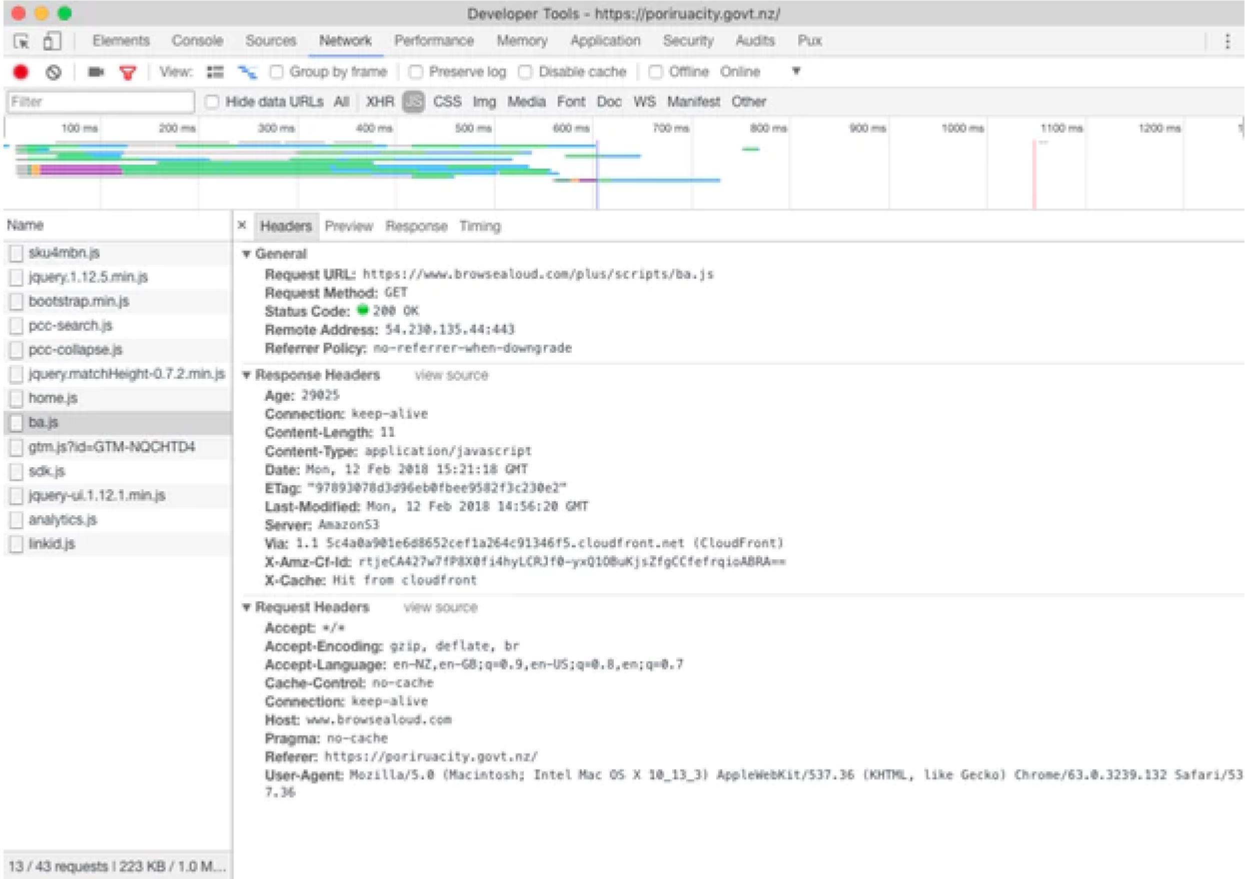
"We were using the third party plugin BrowseAloud to enable people with sight impairments to 'read' our site. BrowseAloud converts website text to audio. Customers who used this plugin load it directly from the Browsealoud website not the Porirua City Council website."

The Whangarei District Council, which is still running the script, has been contacted for comment.

Lyons said this type of hack was sometimes referred to as a "drive-by exploit", when visitors to the site went there for something else but ended up being harmed by something else in the process.

"There are ways to stop these kinds of exploits but it does take time and it does take resource to do that, so sometimes we know when things do slip through ... you find yourself in situations where you put yourselves and the people who use your website potentially in harm's way."

If websites had "holes" and vulnerabilities that allowed such things to happen, then "the world's your oyster as far as the hacker's concerned."



```
sku4mbn.js
jquery.1.12.5.min.js
bootstrap.min.js
pcc-search.js
pcc-collapse.js
jquery.matchHeight-0.7.2.min.js
home.js
ba.js
gtm.js?id=GTM-NQCHTD4
sdk.js
jquery-ui.1.12.1.min.js
analytics.js
linkid.js

13 / 43 requests | 223 KB / 1.0 M...
```

```
▾ General
    Request URL: https://www.browsealoud.com/plus/scripts/ba.js
    Request Method: GET
    Status Code: ● 200 OK
    Remote Address: 54.230.135.44:443
    Referrer Policy: no-referrer-when-downgrade
▾ Response Headers     view source
    Age: 29025
    Connection: keep-alive
    Content-Length: 11
    Content-Type: application/javascript
    Date: Mon, 12 Feb 2018 15:21:18 GMT
    ETag: "97893078d3d96eb0fbee9582f3c230e2"
    Last-Modified: Mon, 12 Feb 2018 14:56:20 GMT
    Server: AmazonS3
    Via: 1.1 5c4a0a901e6d8652cef1a264c91346f5.cloudfront.net (CloudFront)
    X-Amz-Cf-Id: rtjeCA427w7fP8X0fi4hyLCRJf0-yxQ10BuKjsZfgCCfefrqioABRA==
    X-Cache: Hit from cloudfront
▾ Request Headers     view source
    Accept: */*
    Accept-Encoding: gzip, deflate, br
    Accept-Language: en-NZ,en-GB;q=0.9,en-US;q=0.8,en;q=0.7
    Cache-Control: no-cache
    Connection: keep-alive
    Host: www.browsealoud.com
    Pragma: no-cache
    Referer: https://poriruacity.govt.nz/
    User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_13_3) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/63.0.3239.132 Safari/53
    7.36
```

Screenshots show the affected ba.js script still being used on the Porirua City Council website on Tuesday. Image / Chris Knox

"They could be at that point trying to put similar software on your computer that causes a chain reaction across the internet."

Hackers could potentially dig for sensitive details including names, passwords, logins, emails, or, on the more serious end, driver's licence details, passport numbers, and bank details.

Anyone using their banking details on the council website was not at risk from the vulnerability, though, as the parts of the site used for payments were hosted elsewhere.

Lyons said people managing public websites should run firewalls and run systems on the servers, and these would stop 99 per cent of attacks.

In a statement released on Sunday, the third party provider Texthelp confirmed their BrowseAloud script had been compromised in a cyber attack.

"The attacker added malicious code to the file to use the browser CPU in an attempt to illegally generate cryptocurrency. This was a criminal act," said chief technology officer Martin McKay in the statement.

"Texthelp is working with the National Crime Agency and The National Cyber Security Centre to pursue the investigation further."

## Trending on NZ Herald

NEW ZEALAND

### 'Evil' policy robs pensioners of dignity, independence

5 Mar, 2018 5:09pm

4 minutes to read

Three pensioners say their human rights are being breached by pension deductions.

BUSINESS

### US billionaire threatens to halt NZ expansion plans if foreign ban passes

5 Mar, 2018 10:19am

3 minutes to read

Billionaire won't expand in NZ if law change is enacted.

**SPORT**

### Aussie Warner in ugly tunnel fracas

5 Mar, 2018 3:15pm

5 minutes to read

Leaked video has emerged of a spiteful dressing room confrontation in Durban.